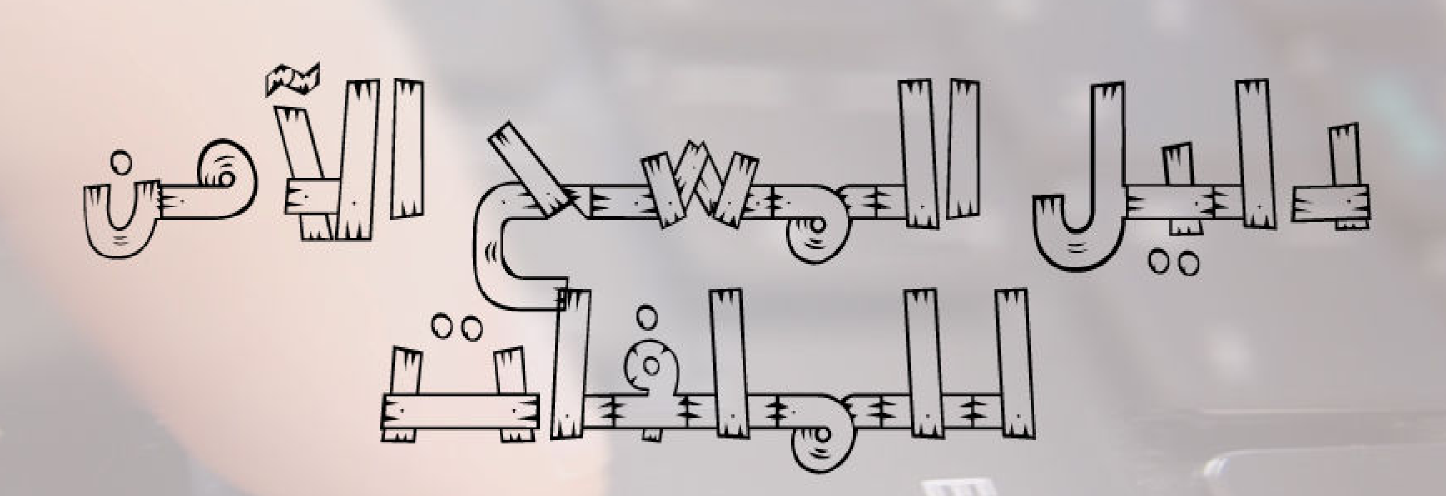




- مسح الملفات بواسطة برامج
- طرق آمنة لمسح الملفات
- ضمان عدم استرجاع الملفات من جديد



منتديات شموخ الإسلام

تمهيد

لاشك أن صورك و ملفاتك الصوتية و المرئية و أسماء و عناوين بريد أو الهاتف و أشياء أخرى على حاسوبك ، تشكل جانبا من حياتك و شخصيتك، لكنك ذات يوم قد ترغب في التحفظ على شخصيتك، و بالتالي منع المتطفلين من الاطلاع على بعض ملفاتك الخاصة، أو ربما بيع حاسوبك، فتقوم بحذفها بنقرة زر، أملا في التخلص منها لغير رجعة، لكن هل حذف الملفات يعني أنك مسحتها نهائيا؟ حتى لو قمت بتفريغ سلة المهملات؟

في الواقع لا، الطرق الكلاسيكية التي نتبعها لمسح الملفات تقوم بالغاء تعريفها فقط وليس المسح الكامل، و يمكن استعمال أدوات خاصة لاسترجاع كافة بياناتك على الحاسوب منها المدفوعة كـPower Date Recovery أو مجانية كـRecuva ، و هنا نتساءل عن الطريقة المثلى للتخلص من الملفات بشكل آمن يضمن عدم استرجاعها بأي برنامج أو طريقة، و هذا موضوعنا اليوم في العدد الأول من دليل الأنصار، و الذي يجب أن نراعي فيه عند القراءة الفرق بين الحذف و المسح، الحذف يشبه إخفاء الملفات أكثر من الحذف الفعلي، أما المسح نقصد به مسح الملفات دون القدرة على استرجاعها ثانية.

و الله ولي التوفيق.

أبو مصعب الضحاك

في هذا العدد




```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Mike Fagan>format /?
Formats a disk for use with Windows.

FORMAT volume [/FS:file-system] [/V:label] [/Q] [/A:size] [/C] [/X] [/P:p
[/S:state]
FORMAT volume [/V:label] [/Q] [/F:size] [/P:passes]
FORMAT volume [/V:label] [/Q] [/T:tracks /N:sectors] [/P:passes]
FORMAT volume [/V:label] [/Q] [/P:passes]
FORMAT volume [/Q]
```

يعد الفورمات من أنجع الحلول بالنسبة لمستعمل الحاسب المبتدئ و حتى المتوسط في بعض الأحيان، للتخلص من الملفات بأمان، مما يمكن القيام به في هذا الصدد، التهيئة العالية المستوى High Level Format ويشار إليها بـ التهيئة السريعة Quick Format، وهذه الطريقة ليست آمنة، لأنها تقوم فقط بحذف قطاعات الإقلاع Boot Sectors و جدول القسم Partition Table، لهذا فالملفات التي نريد التخلص منها، لازال بالإمكان استرجاعها و لازال خطر العبث بها وارد.

هنالك أيضا التهيئة المنخفضة المستوى Low Level Format و يشار إليها بإعادة تهيئة القرص الصلب Disk Reinitialization وهذه العملية تقوم بمسح كامل البيانات التي بالقرص الصلب، و بالنسبة لمستخدم الحاسب المتقدم، يمكنه تغيير عدد أدوار المسح Number of Passes، و كل ما زاد عددها كان أفضل لتأمين مسح الملفات و الكتابة عليها مما يزيد من صعوبة استرجاعها و زيادتها أيضا تعني وقتا أطول لإجراء العملية.

مما سبق يبدو لك أنها الطريقة الثانية هي المثلى، لكن هنالك بعض الفخاخ، كأن تقوم بالتهيئة بنظام مغاير للذي كان في القرص الصلب أو تقسيمه إلى عدة أقسام Partitions، في هذه الحالة البيانات لا تمحى بالكامل.

إذن تهيئة القرص الصلب ليست بالطريقة الممتازة التي تمكنك من مسح الملفات لغير رجعة، عوضا عن بعض الأدوات الفعالة التي سنتطرق لبعضها لاحقا في هذا الدليل.

و للاستزادة في مجال الفورمات وأ نظمته راجع الكتيب الموجود على الرابط:

http://www.archive.org/download/HowToFormatUsbDiskDrive/FormatHdUsb32gb.pdf

مسح الملفات بواسطة برنامج Darik's Boot And Nuke



برنامج DBAN مجاني و حجمه صغير، لكنه كفؤ في مجال المسح الآمن للملفات.

الموقع الرسمي للبرنامج :

http://www.dban.org

صفحة التحميل:

http://www.dban.org/download

Darik's Boot And Nuke

Download | Help | News | Contact | About DBAN
SourceForge Project Page | Development Status | Documentation

Home

DBAN Download

Preview Releases

- DBAN 2.2.6 Beta for CD-R and DVD-R media.
  (Burn this file to a blank disc and boot the computer with it. Do not unzip this file.)

See Also

- Old Releases, Alternate Downloads, and Source Code

Complementary Products

- Use TrueCrypt for full volume encryption.
- Use Heidi Eraser for file wiping within the Microsoft Windows environment.



قم بتحميل صورة البرنامج ISO وقم بحرقها على قرص مرن، ثم أدخله في سواقة قارئ الأقراص، وقم بإعادة تشغيل الحاسوب restart قصد الإقلاع من القرص المرن الذي حرقنا عليه البرنامج، قد تحتاج للضغط على الزر F12 لهذا الأمر. عند ظهور شاشة البيوس BIOS وهي الشاشة التي تظهر حال تشغيل الحاسوب، ثم الخيار Boot from your CD/DVD، وبعد ذلك ستظهر الشاشة أسفله:

```
Darik's Boot and Nuke

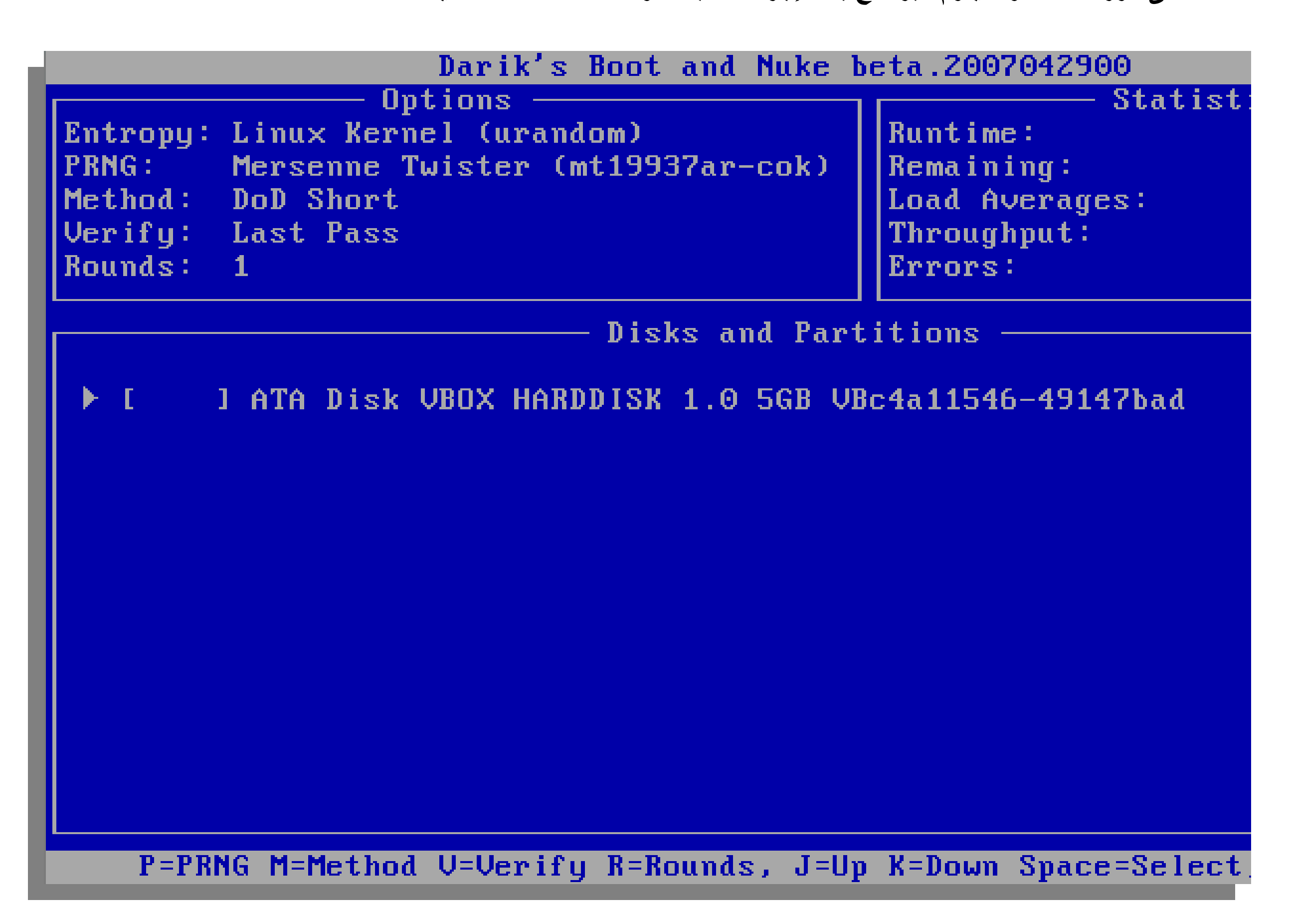
Warning: This software irrecoverably destroys data.

This software is provided without any warranty; without even the
warranty of merchantability or fitness for a particular purpose
shall the software authors or contributors be liable for any dar
from the use of this software.  This software is provided "as is

http://www.dban.org/

* Press the F2 key to learn about DBAN.
* Press the F3 key for a list of quick commands.
* Press the F4 key for troubleshooting hints.
* Press the ENTER key to start DBAN in interactive mode.
* Enter autonuke at this prompt to start DBAN in automatic mode
```

اضغط على الزر Enter و سيقوم البرنامج بعدة إجراءات قبل التوقف عند الشاشة التالية:



اضغط على الزر مساحة Space عندما يظهر لك بين] [كما في الصورة أعلاه الحرف المميز للقسم Partition أو القرص الذي تريد حذف بياناته بشكل نهائي لاختياره، ثم اضغط على الزر F10 لبدء العملية.

وستظهر لك شاشة كالتي بالأسفل.

```
Darik's Boot and Nuke beta.2007042900
Options
Entropy: Linux Kernel (urandom)
PRNG:    Mersenne Twister (mt19937ar-cok)
Method:  DoD Short
Verify:  Last Pass
Rounds:  1

Statisti
Runtime:        00:00
Remaining:
Load Averages: 0.47
Throughput:
Errors:         0

ATA Disk VBOX HARDDISK 1.0 5GB VBc4a11546-49147bad
  [02.20%, round 1 of 1, pass 1 of 3] [writing] [0 B/s]
```

و انتظر القيام بالعملية إلى غاية ظهور شاشة تعلمك بانتهاء المهمة، كهذه.

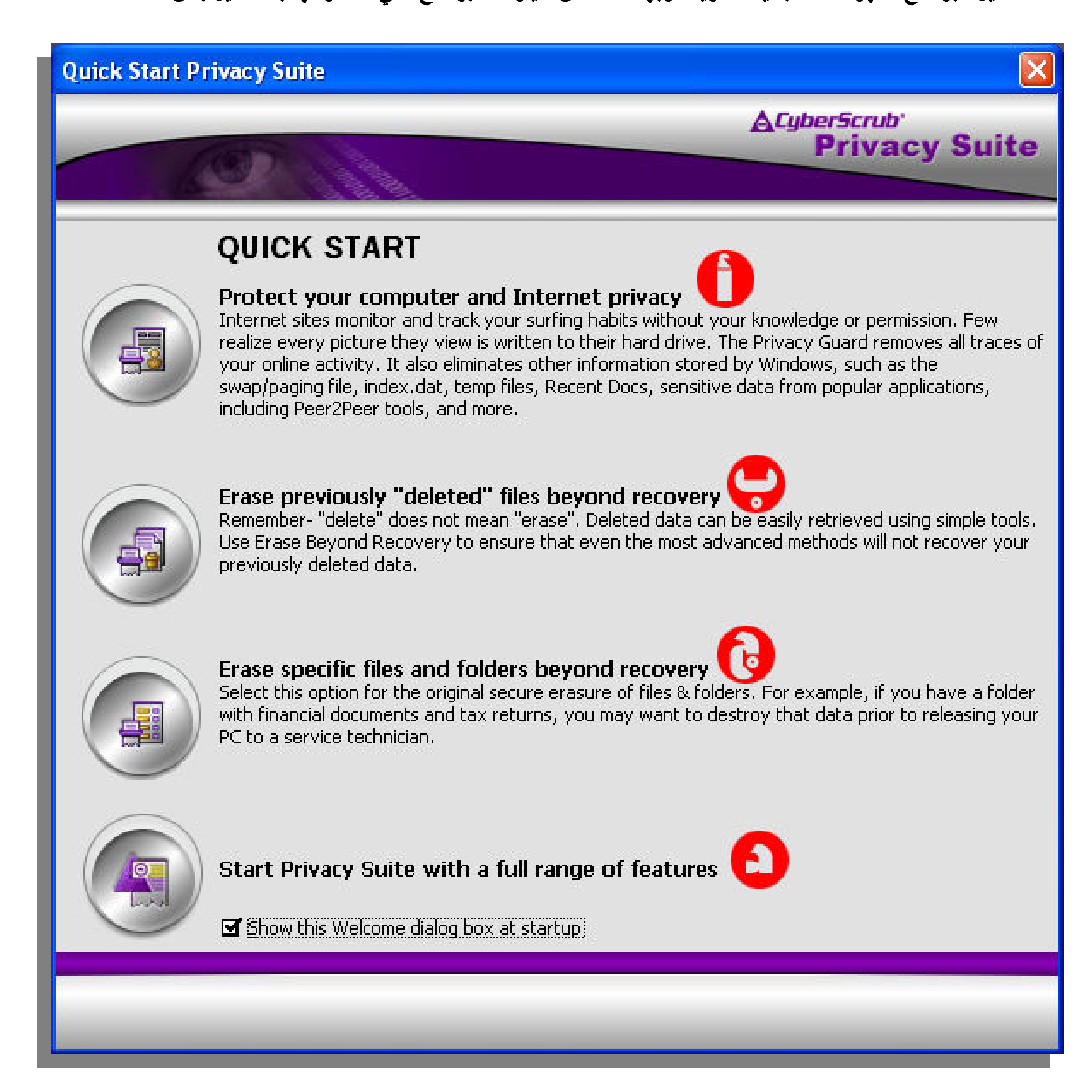
```
DBAN succeeded.
All selected disks have been wiped.
Hardware clock operation start date:  Tue Mar 16 14:31:17 2010
Hardware clock operation finish date: Tue Mar 16 14:48:44 2010
Saving logs to A:\DBANLOG on removable media... done.
_
```

الموقع الرسمي للبرنامج:

http://www.cyberscrub.com

برنامج CyberScrub غير مجاني، لكنه ممن أقوى البرامج في مجال التخلص من الملفات، و يحتوي على مزايا كثيرة، لا توجد بغيره من البرامج، وهي ما سنكتشف بعون الله في هذا الشرح.

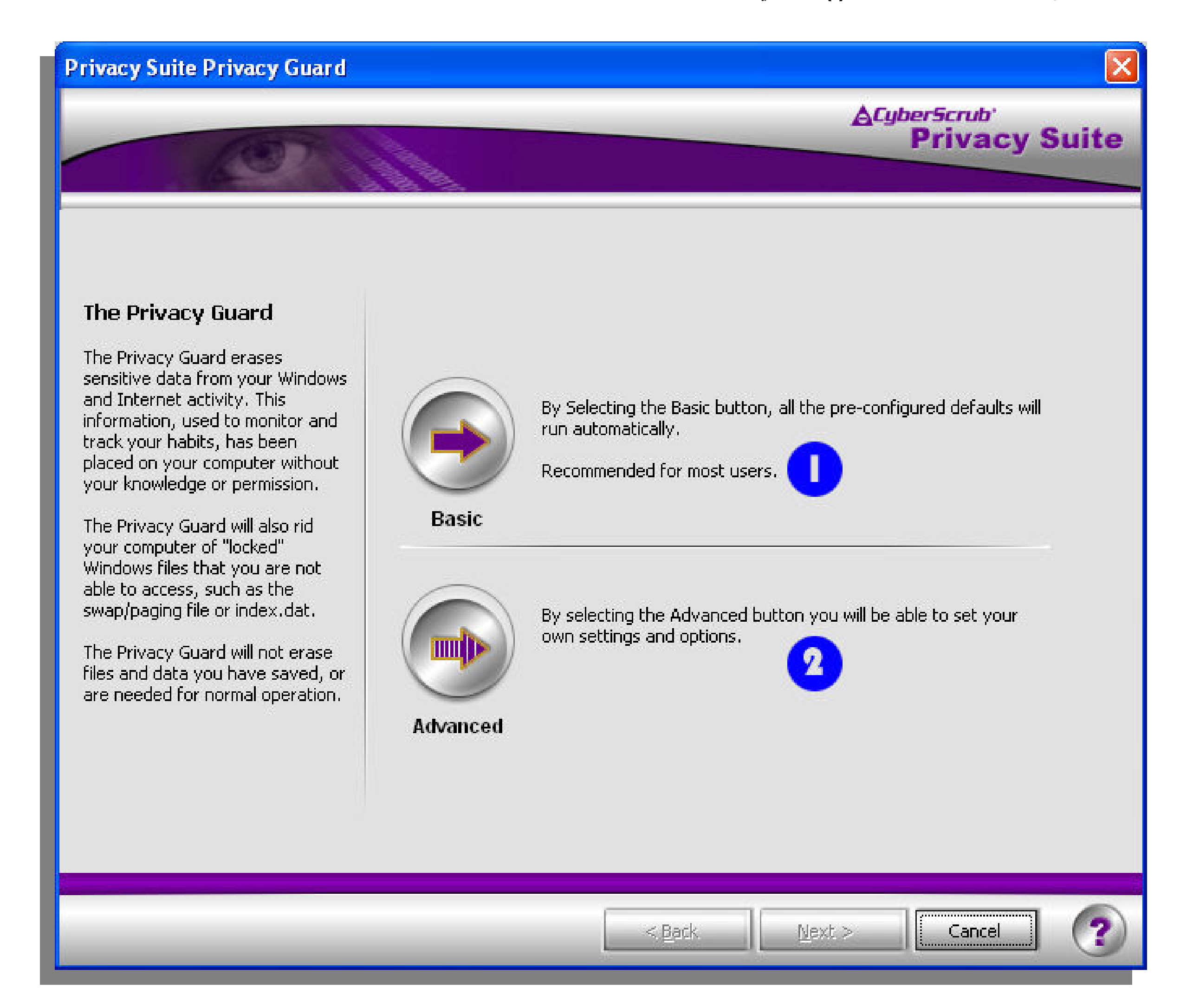
عند تشغيل البرنامج تظهر نافذة البداية السريعة وبها قائمة من خيارات البرنامج التي سنشرحها بالتفصيل باذن الله.



أ. Protect your computer and Internet privacy

من خلال الخيار (أ) يمكن حماية خصوصيتنا بعد الإبحار في الانترنت، عن طريق مسح كل الآثار الدالة علينا، و كذلك مخلفات النظام و مخلفات البرامج المتواجدة عليه، التي قد تشكل خطرا على أمننا الشخصي.

نضغط على القرص المقابل للخيار (أ) كما في الصورة أعلاه، فتظهر النافذة التالية:



1- للمسح القياسي

2- للمسح المتقدم

و سنختار المسح المتقدم حتى نتحكم بالإعدادات و ذلك بعد الضغط على القرص الذي بداخله سهم أعلى كلمة Advanced.



هنا قائمة العناصر الهدف، التي سيتم مسح بعض مكوناتها التي تضر بأمننا الشخصي وهي كالتالي:

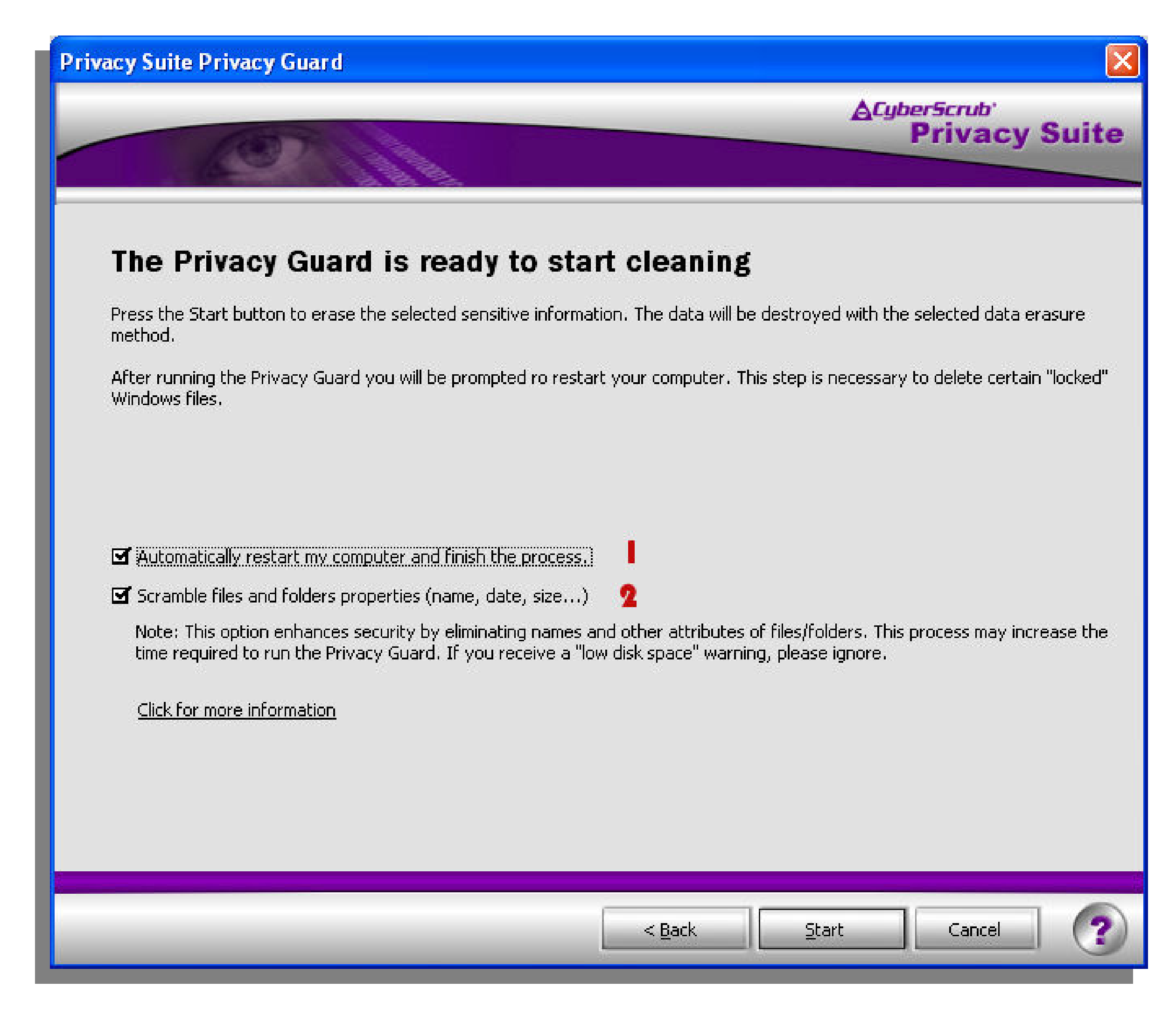
- الوندوز Windows : هذا الخيار يمكن من مسح جميع الملفات الضارة بالخصوصية التي يضعها النظام، مثل آخر الملفات التي تصفحتها و الملفات المؤقتة التي تضعها البرامج، إلى غير ذلك.
- متصفحات الانترنت Browsers: استعمل هذا الخيار لمسح آثار تصفحك للانترنت بواسطة المتصفحات كـ FireFox مثلا.
- Peer2Peer : هذا الخيار لمسح البيانات الضارة بأمنك الصادرة عن برامج التحميل بتقنية Peer2Peer كبرامج التورنت من Utorrent و Ares وغيرها من البرامج.
- News & Email Readers : مسح البيانات الضارة الصادرة عن برامج قراءة الايميلات كبرنامج thunderbird و أنشطتك عبر المجموعات الإخبارية.
- Custom : لاضافة برامج أخرى غير واردة في هذا الإصدار.

اضغط على كلمة Next > لتظهر النافذة التالية :



العناصر المستهدفة: كما ذكرنا سابقا.

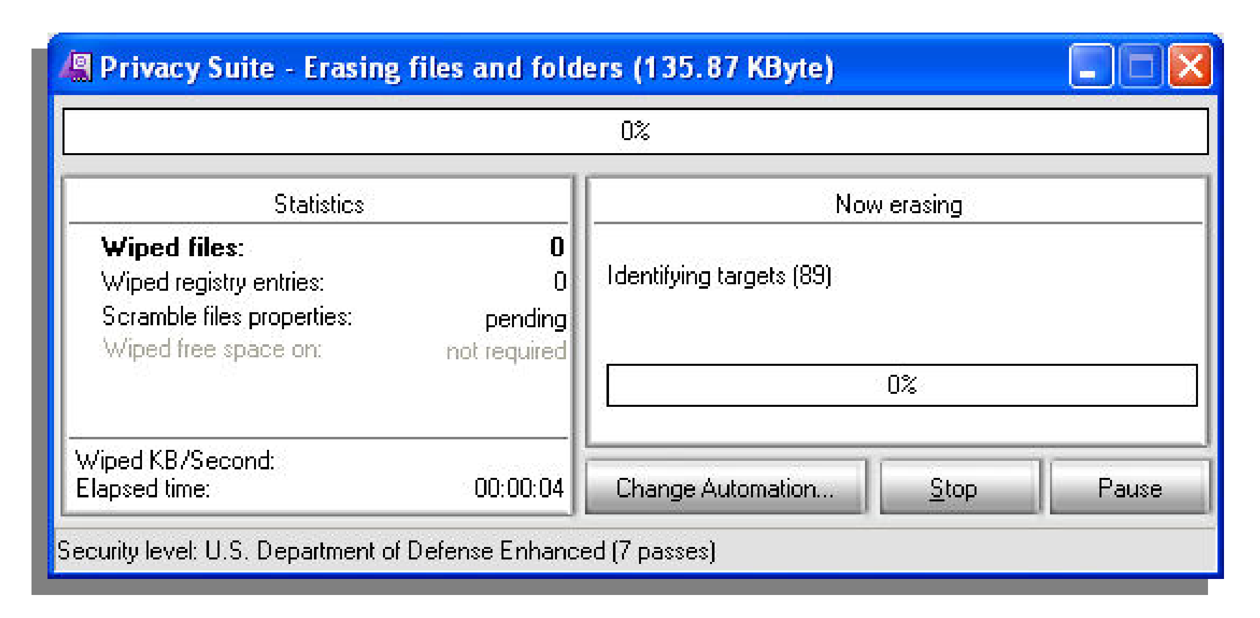
قائمة إعدادات العناصر المستهدفة : عند التأشير على المربع الصغير بجانب كل خيار، تكون قد أعطيت الأمر لبرنامج CyberScrub بمسح الملفات الضارة التي يطرحها ذلك البرنامج.



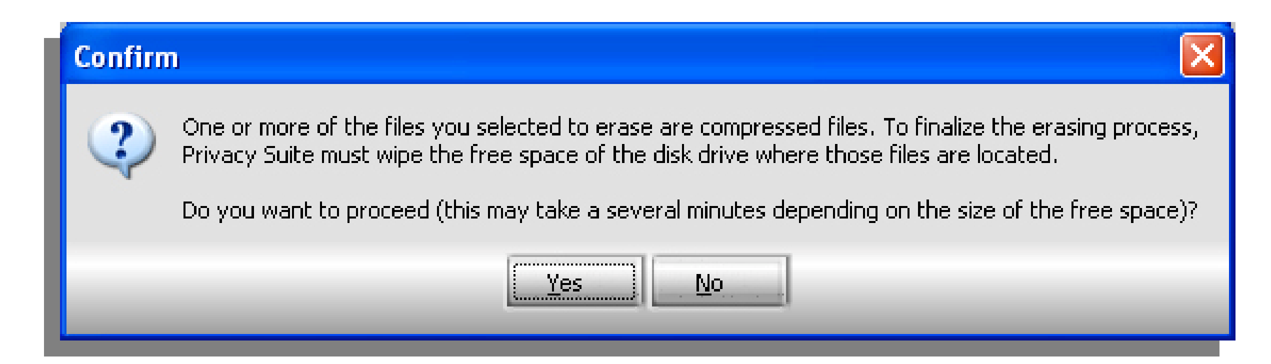
التأشير على الخيار 1 يعني إعادة تشغيل الحاسوب لإكمال مهمة مسح الملفات.

الخيار 2 يقوم ببعثرة خصائص الملفات كالاسم و التاريخ و الحجم، هذا الخيار مهم للغاية لزيادة أمنك الشخصي، لأنه يمكن من زيادة صعوبة استرجاع الملفات، قد تظهر لك رسالة تنبهك بأن القرص الصلب ممتلئ أثناء تشغيل هذا الخيار في عملية الحذف، فلا تعره اهتماما. فالبرنامج يقوم بملئ القرص ببيانات قصد بعثرة خصائص الملفات.

اضغط على Start لبدء عملية المسح.



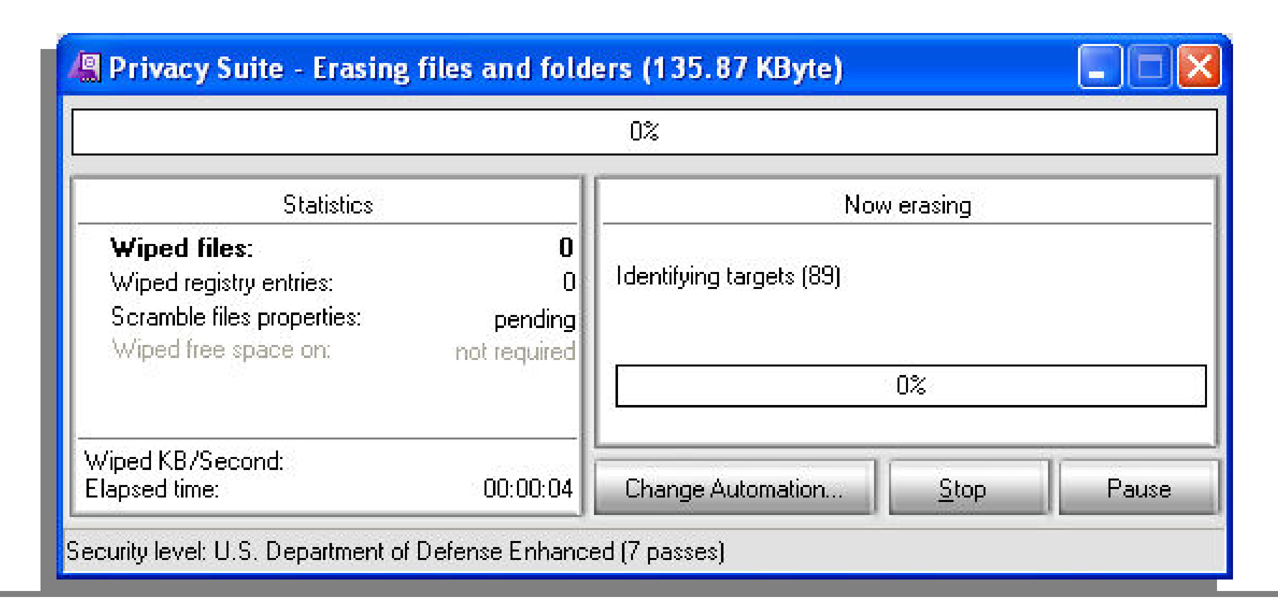
ستظهر هذه النافذة و بعدها قد تصادفك النافذة التالية:



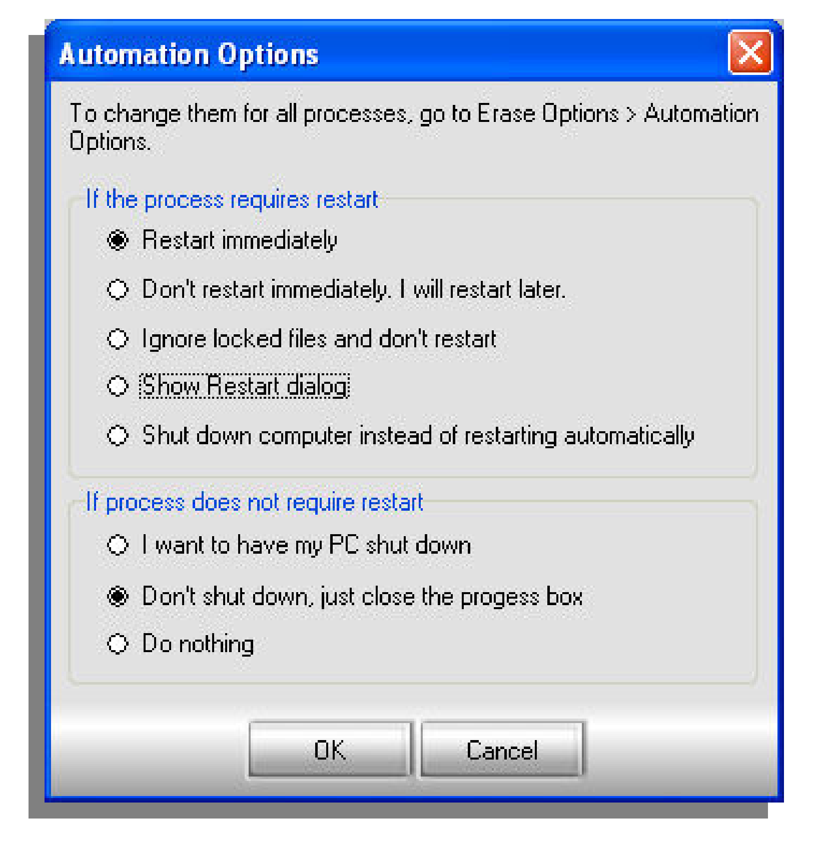
هنا يطلب منك البرنامج تحديد رغبتك في مسح المساحات الفارغة في القرص الصلب.

المساحة الفارغة هي الجزء الذي لا يوجد به ملفاتك لكنه في الواقع يحوي ملفات محذوفة سابقا، و يقوم البرنامج بالكتابة على هذه المعلومات لزيادة صعوبة استرجاعها و إتلافها، و ذلك عن طريق خوارزميات و أدوار الحذف Passes، كلما زاد عدد الأدوار Passes كلما زادت صعوبة استرجاع الملفات، وسنرى كيف يمكننا التحكم في عدد الأدوار لاحقا في هذا الشرح.

بعد حسم خيارك ستختفي النافذة و نعود لنظيرتها السابقة:



اضغط على خيار Change Automation وسترى النافذة التالية التي تعطيك خيارات بعد الانتهاء من المسح الأولي للملفات:



في حال طلب البرنامج إعادة التشغيل:

- إعادة التشغيل على الفور لاستكمال المسح **Restart immediately.**
- إلغاء إعادة التشغيل الفوري، واستكمال المسح بعد تشغيل الحاسوب **Don't restart immediately. I will restart later .**
- تجاهل الملفات المغلقة مع عدم إعادة تشغيل الحاسوب **Ignore locked files and don't restart.**
- إظهار نافذة خيارا إعادة التشغيل **Show Restart dialog .**
- غلق الحاسوب عوضا عن إعادة تشغيله.

في حال عدم طلب البرنامج إعادة التشغيل:

- غلق الحاسوب **I want to have my PC shut down.**
- الإبقاء على الحاسوب مشغلا مع غلق نافذة الاستمرار.
- الإيعاز للبرنامج بألا يقوم بشيء.

ب. Erase previously « Deleted » files beyond recovery

هذا الخيار يمكننا من مسح الملفات المحذوفة بالطريقة الكلاسيكية و التي يمكن استرجاعها بأدوات بسيطة.

اضغط على الخيار (ب) كما في الصورة في أول هذا الشرح، لتظهر النافذة التالية:



تحديد العناصر المتسهدفة:

- تحديد وسائط التخزين التي ستجرى عليها عملية المسح سواءا كان قرصا صلبا أو مفتاح USB أو غيرها من وسائط التخزين.
- **Destroy all files from the Recycle Bin beyond recovery**

قم بالتأشير على هذا الخيار لمسح الملفات المتواجدة بسلة المحذوفات بشكل نهائي.

- **Eliminate the deleted information on the following**

التأشير على هذا الخيار ضروري لاجراء عملية المسح.

خيارات مسح الملفات:

- **Wipe the free (unused) disk space**

مسح المساحات الفارغة بالقرص الصلب.

- Wipe the slack of existing files

مسح الملفات المهملة، هذا الخيار مهم جدا لكنه يسبب بعض البطء في للجهاز.

- Scramble deleted files and folders properties

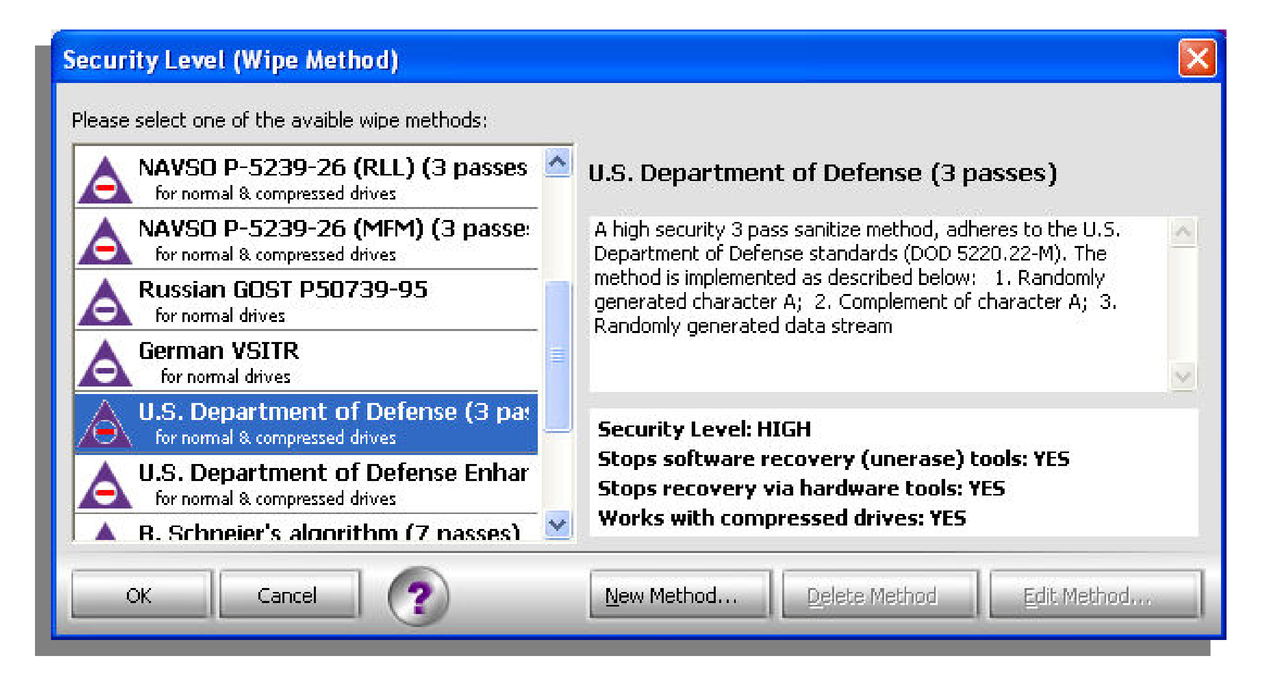
بعثرة خصائص الملفات كالاسم و التاريخ و الحجم الى غير ذلك.

- Scramble system transactions log file

بعثرة ملفات الـ Log ، أشر على هذا الخيار إذا كان القرص الصلب خاصتك يعمل بنظام NTFS.

اختيار نظام المسح Erasure Settings:

اضغط على الزر Erasure Settings لتظهر النافذة التالية:



على اليسار مختلف أنظمة المسح المتوفرة، النظام الافتراضي هو U.S Departement of Defense، و الكثير من مستعملي البرنامج عند رؤية هذا الاسم يظنون أن البرنامج من صنع وزارة الدفاع الأمريكية و هذا خطأ، هو فقط النظام الافتراضي، ويوجد غيره في القائمة على اليسار.

نلاحظ أن النظام الافتراضي يتكون من 3 أدوار 3 Passes و أسفله نفس النظام لكن بـ 7 أدوار و كلما زاد عدد الأدوار، كان مسح الملفات أكثر أمنا، إلا أن زيادة عدد الأدوار تعني أيضا وقتا أكثر تأخذه عملية المسح.

اختر النظام الذي تريد و اضغط على ok، بإمكانك أن تغير النظام كل مرة عند كل مسح جديد.

أولوية البرنامج Priority Settings:

للتحكم في حصة البرنامج من موارد الذاكرة العشوائية الـRam و المعالج، يستحسن ألا يعدل هذا الخيار و أن يترك كما هو.

ج. Erase specific files and folders beyond recovery

انطلاقا من هذا الخيار يمكننا مسح ملفات متواجدة على وسائط التخزين كالقرص الصلب مثلا بشكل نهائي، لأننا فيما سبق تحدثنا عن مسح الملفات المحذوفة و ليس التي لازالت تتواجد على الجهاز.

بعد الضغط على الزر كما في الصورة في أول هذا الشرح، ستظهر هذه النافذة الصغيرة.



الخيار الأول لاختيار ملف و الثاني لاختيار مجلد للمسح.

اضغط ok مع خيار الملف و ستظهر لك نافذة لتحديد مكان تواجده في حاسوبك.

Select the file(s) you want to erase

Regarder dans : Poste de travail

Recent
Bureau
Mes documents
Poste de travail
Favoris réseau

Disquette 3½ (A:)
Disque local (C:)
Disque local (D:)
Disquel local (E:)
Lecteur DVD-RAM (F:)
Lecteur DVD (G:)
Documents partagés
Documents de Administrateur

Nom du fichier : WinRAR.lnk
Fichiers de type : All Files
Ouvrir
Annuler

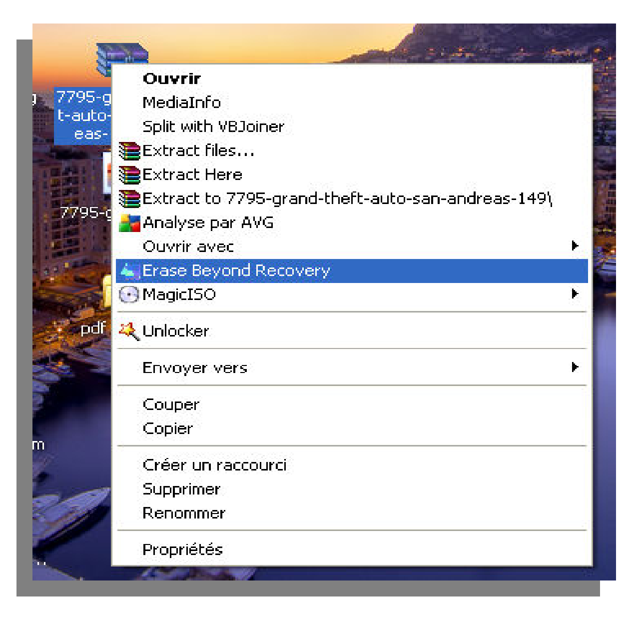
حدد الملف الذي تريد مسحه، وسيضاف الى القائمة، اضغط بالزر الأيمن للفأرة في مكان فارغ لتظهر القائمة كما في الصورة أسفله.



بعد الانتهاء من تحديد الملفات أو المجلدات التي ترغب في مسحها. اضغط على الزر **Erase All** الموجود يسارا.

أو من أسفل القائمة عن الضغط في المساحة البيضاء بيمين الفأرة.

يمكنك أيضا الصغط يمين الفأرة على الملف الذي تريد مسحه او المجلد، أو عدة ملفات تقوم بتظليلها كما في الصور أسفله:



واضغط على **Erase All** كما ذكرنا آنفا.



لتحميل البرنامج، راجع أحد الروابط الموثوقة التالية، واحذر من النسخ المقلدة للبرنامج، التي بها وسائل تجسس تطرح من جهات غير رسمية:

http://202.149.72.130/~shamikh/vb/showthread.php?t=96252

http://shamikh1.net/~shamikh/vb/showthread.php?t=96252

نفتح برنامج أسرار المجاهدين، و هذ هي واجهته الرئيسة :

Ekhlaas Network
MOJAHEDEEN SECRETS
Version 2.0

Encrypt File
Decrypt File
Sign / Verify
Messaging
Keys Manager
File Shredder
Preferences
About
Exit

Anti-Symmetric Keys

Type	User ID	Key ID	Length	Creation

Remote User (Public Key) Key ID Clear Key
Local User (Private Key) Key ID Clear Key
Symmetric Cipher Algorithm: Rijndael with 256 bit key (AES)
Stealthy Cipher: Activate Stealthy Cipher
t File to Encrypt | Select File to Decrypt | File Encoding and Deco
Path: Select...
Shred Out Original File. Sign Encrypted File.

نضغط على الزر Preferences كما في الصورة أعلاه، فتنبثق النافذة التالية :

مستويات الضغط

عدد أدوار المسح، كلما زاد عددها زادت صعوبة استرجاع الملف الممسوح، لذا ينصح بتركها في القيمة 10 التي هي أقصى ما يمكن لبرنامج أسرار المجاهدين فعله بهذا الصدد

Preferences

Compression Level

Fastest Compression

No Compression (Disabled)
Fastest Compression
Normal Compression
Maximum Compression (Slowest)

...ession for documents and files
...st compression or disable it.

File Shreddering

Number of times files are wiped out 10

Help OK Cancel

مستويات الضغط :

- No compression (Disabled) أي مسح الملفات بدون ضغط
- Fastest Compression ضغط سريع
- Normal Compression ضغط عادي
- Maximum Compression ضغط قصوي

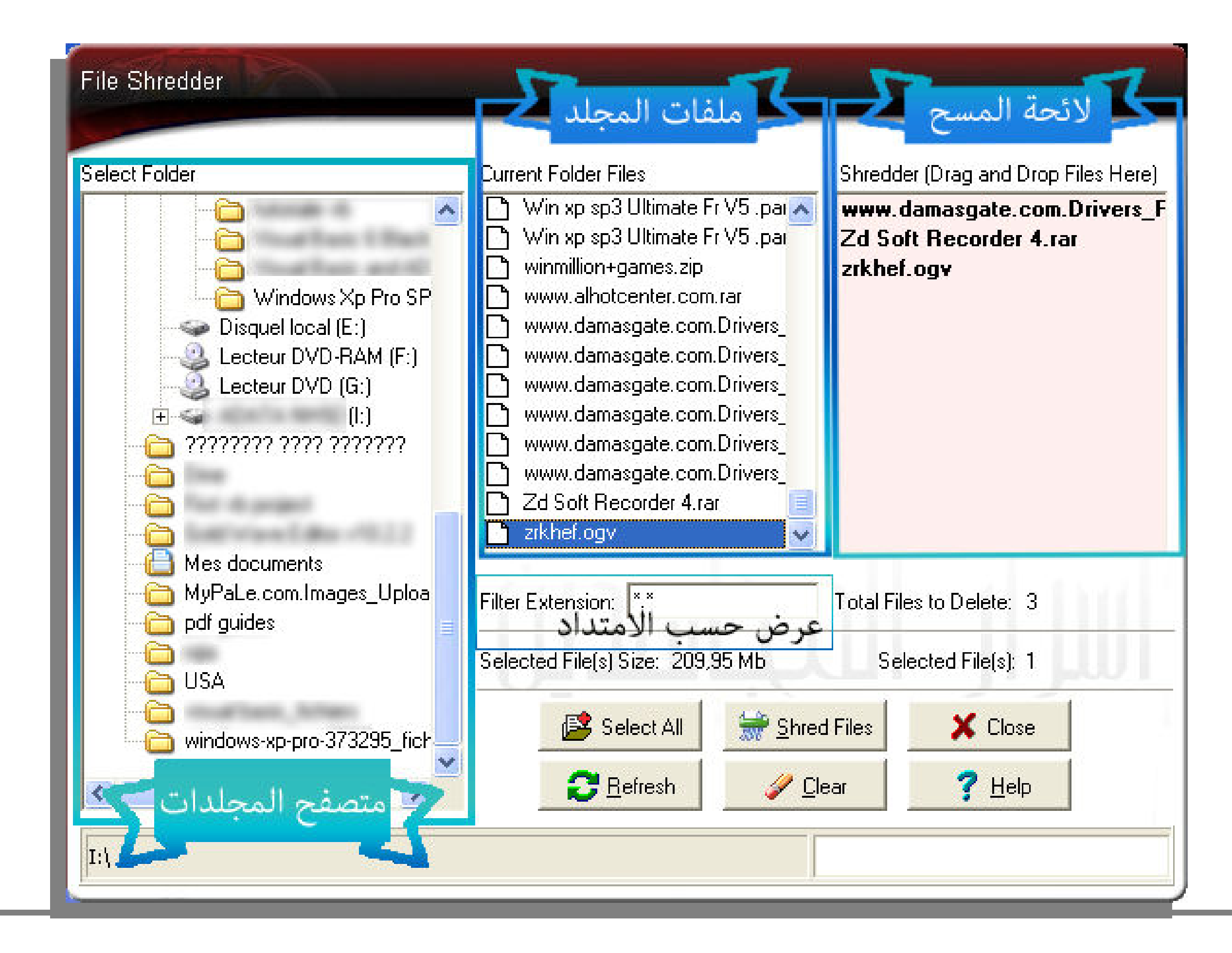
- بالنسبة للملفات التي حجمها أقل من 10 ميغا بايت، ينصح باستعمال مستوى الضغط القصوي Maximum Compression.
- أما للملفات الكبيرة الحجم، استعمل الضغط السريع Fastest Compression أو لا تستعمل أي ضغط أي الخيار No compression (Disabled).

بعد اختيار إعداداتك المفضلة، اضغط على الزر 

و نعود إلى الواجهة الرئيسية للبرنامج، ثم نضغط على الزر File Shredder كما هو مشار إليه في الصورة بالأسفل.

Ekhlaas Network
MOJAHEDEEN SECRETS
Version 2.0
Anti-Symmetric Keys
Type | User ID | Key ID | Length | Creation
Remote User (Public Key) | Key ID | Clear Key
Local User (Private Key) | Key ID | Clear Key
Encrypt File
Decrypt File
Sign / Verify
Messaging
Keys Manager
File Shredder
Preferences
About
Exit
tric Cipher Algorithm
ndael with 256 bit key (AES)
Stealthy Cipher
Activate Stealthy Cipher
Select File to Encrypt | Select File to Decrypt | File Encoding and Deco
Path: | Select...
Shred Out Original File. | Sign Encrypted File.

و ستظهر النافذة التالية :



متصفح المجلدات: يستعرض المجلدات التي بالحاسوب و وسائط المتصلة به، و منه تحدد المجلد الذي تريد مسح الملفات المتواجدة عليه.

متصفح المجلد: يستعرض الملفات التي يحويها المجلد الذي اخترته من متصفح المجلدات.

لائحة المسح: الملفات التي سيمسحها البرنامج، ولا ختيار ملف للمسح اضغط مرتين عليه في متصفح المجلد أو قم بسحبه فوق لائحة المسح.

عرض حسب الامتداد: استعراض الملفات حسب امتداد معين، مثلا أريد أن تظهر على متصفح المجلد ملفات صوتية MP3 فقط حينها أقوم بكتابة MP3.* بدل *.*



Select All: لاختيار جميع الملفات التي بالمجلد لمسحها.

Shred Files: بدء عملية المسح.

Close: خروج من النافذة.

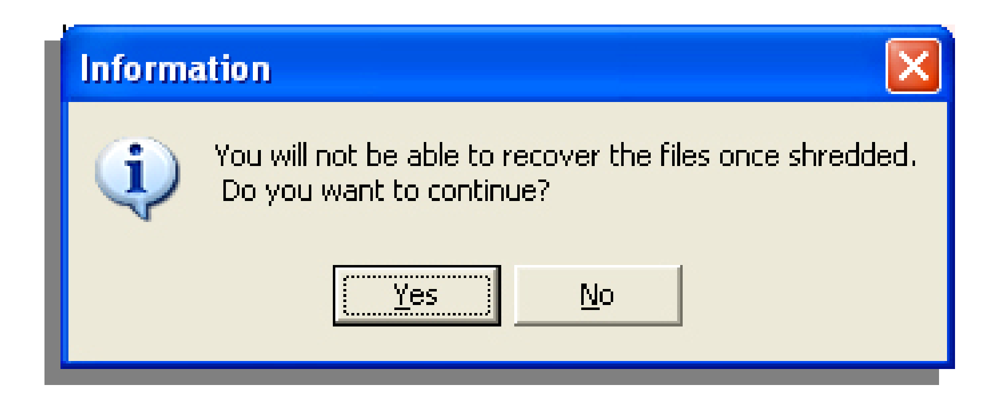
Refresh: تحديث ملفات المتصفح.

Clear: إفراغ لائحة المسح من محتواها دون مسح الملفات.

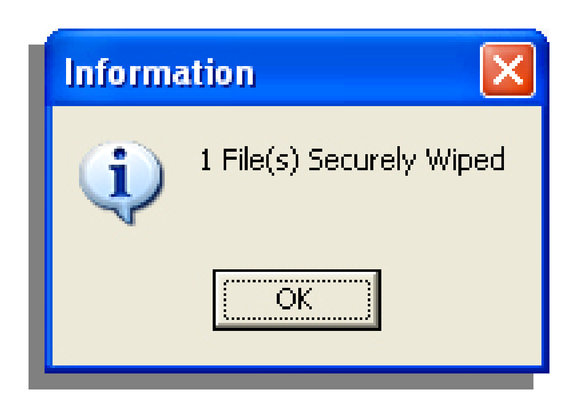
Help: قراءة ملف المساعدة.

بعد اختيار الملفات التي تريد مسحها، اضغط على الزر Shred Files لبدء عملية المسح.

ستظهر لك النافذة التالية لتأكيد خيارك بالمسح:



اضغط Yes وستظهر النافذة التالية، تعلمك بنجاح العملية:





التخلص من الملفات يدويا



تعد الطريقة الأمثل لضمان مسح الملفات نهائيا، و ذلك بتدمير القرص الصلب، وهنالك طرق أخرى كفيلة بهذا الأمر.

قم بتقريب مغناطيس ذو طاقة عالية High Powered Magnet من القرص الصلب عدة مرات، و سيقوم بخلط البيانات التي بالقرص الصلب خاصتك.

و هناك خيار أخر بعد أخذ الاحتياطات الوقائية كارتداء نظارات واقية قم بفك القرص الصلب بواسطة مفك البراغي نوع T9 torx ثم بواسطة مطرقة حطم القرص و لا تبقي منه أي شيء.

بإمكانك أيضا الاستعانة بالمثقاب الكهربائي Driller و ثقب القرص الصلب، واصنع عدة ثقوب في الغلاف المعدني.

مسك الختام

و في الختام أشكر الأخ أبو عمر الشاميTime Of Terror ، ميسرة، حيدرة، جلمود الإسلام، Song OF Terror و غيرهم ممن لا يحضرني ذكرهم، ولهم أهدي هذا العمل، الذي أسأل الله أن يبارك فيه و يتقبله مني، وأن يعينني على الاستمرار فيه، كما أتمنى من الإخوة دعم الدليل بمشاركاتهم فيه، و إسداء النصح و التوجيه.

لا تنسوني من صالح دعائكم بالمغفرة و الشهادة.

أخوكم طالب الغفران و الشهادة أبو مصعب الضحاك.

تم بحمد الله.